

SOMMARIO

PRESENTAZIONE	V
----------------------------	---

INDICE AUTORI	XV
----------------------------	----

I PRINCIPI IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI

1. L'AMBITO DI APPLICAZIONE	3
1.1. Introduzione	3
1.2. Ambito di applicazione materiale	4
1.3. Ambito di applicazione territoriale	9
2. IL RISPETTO DEI PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI	16
2.1. Introduzione	16
2.2. Liceità, correttezza e trasparenza	16
2.3. Limitazione della finalità	20
2.4. Minimizzazione dei dati	22
2.5. Esattezza	23
2.6. Limitazione della conservazione	24
2.7. Integrità e riservatezza	25
2.8. Responsabilizzazione o "accountability"	26
3. INDIVIDUAZIONE DELLE BASI GIURIDICHE PER IL TRATTAMENTO	29
3.1. Premessa	29
3.2. Il consenso	31
3.3. Necessità di esecuzione di un contratto	39
3.4. L'adempimento di un obbligo legale	41
3.5. La salvaguardia di interessi vitali	41
3.6. L'esecuzione di un compito di interesse pubblico	42
3.7. Il legittimo interesse	43
4. I DIRITTI DEGLI INTERESSATI	46
4.1. Premessa	46
4.2. Informazioni sul trattamento	47
4.3. Modalità di esercizio dei diritti dell'interessato	50
4.4. I diritti dell'interessato	53
4.5. Limitazioni all'esercizio dei diritti dell'interessato	69

GLI ADEMPIMENTI NELL'ORGANIZZAZIONE INTERNA

5. IL DATA PROTECTION OFFICER O RESPONSABILE DELLA PROTEZIONE DEI DATI	73
5.1. Introduzione: la figura del DPO	73
5.2. Quando nominare un DPO	74
5.3. Come scegliere il DPO e chi nominare	79

5.4.	Il ruolo del DPO all'interno dell'organizzazione del titolare o responsabile del trattamento	81
5.5.	Funzione e compiti del	85
6.	IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO	87
6.1.	Premesse.....	87
6.2.	La tenuta del registro: tra obbligo e opportunità	88
6.3.	Il contenuto del registro	89
6.4.	Modalità di raccolta, conservazione e aggiornamento delle informazioni	93
7.	LA CONSERVAZIONE DEI DATI	95
7.1.	Premesse.....	95
7.2.	La data retention policy.....	96
7.3.	...E le altre procedure.....	98
7.4.	L'informativa agli interessati.....	100
8.	SISTEMA DI GESTIONE DELLA PROTEZIONE DATI (SGPD) IN AZIENDA	101
8.1.	Introduzione	101
8.2.	Cosa è un SGPD	103
8.3.	Componenti di base di un SGPD per conformità al GDPR.....	110
8.4.	Considerazioni sul piano di implementazione di un SGPD.....	132
8.5.	Rapporti del team privacy in azienda.....	135
8.6.	SGPD in uso.....	140
8.7.	Aggiornamento del SGPD	149
8.8.	Conclusioni	151
9.	DIRITTO DEL LAVORO E PRIVACY	154
9.1.	Il rapporto di lavoro tra potere di controllo e tutela della riservatezza	154
9.2.	Il quadro normativo	155
9.3.	Il controllo diretto dei dipendenti	156
9.4.	I controlli a distanza	161
9.5.	Le garanzie procedurali	163
9.6.	Gli strumenti del controllo a distanza.....	164
9.7.	I controlli difensivi	164
9.8.	Il trattamento dei dati personali nel rapporto di lavoro	166
9.9.	Finalità del Codice e definizioni	167
9.10.	Ruolo e obblighi del datore di lavoro	172
9.11.	Diritto di accesso ed azioni del lavoratore	174
9.12.	Gli ambiti di intervento del Garante Privacy.....	175
9.13.	Internet e Posta elettronica	176
9.14.	I dati biometrici del lavoratore.....	178
9.15.	Il necessario coordinamento tra il Codice Privacy e le altre norme del diritto del lavoro	178
9.16.	La tutela dei dati personali dei lavoratori ai tempi del Covid-19	179

VALUTAZIONE E GESTIONE DEL RISCHIO

10. PRIVACY BY DESIGN E BY DEFAULT	185
10.1. Premessa	185
10.2. Il principio di privacy by default	187
10.3. Il principio di privacy by design	190
10.4. Privacy engineering: le strategie per incorporare la privacy nel design dei trattamenti	194
10.5. Data monetization e privacy: come sbloccare il valore dei dati	198
11. LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI	206
11.1. Cos'è e quando serve la DPIA	206
11.2. Ruoli e contenuti	208
11.3. La consultazione preventiva	213
12. LE MISURE DI SICUREZZA E CYBERSECURITY	215
12.1. Principi generali - misure tecniche ed organizzative	215
12.2. Adeguatezza delle misure di sicurezza	219
12.3. Gli standard ISO	220
12.4. Cybersecurity	221
13. CODICI DI CONDOTTA E CERTIFICAZIONI	230
13.1. Premessa	230
13.2. I codici di condotta	230
13.3. Le forme di autoregolamentazione dalla previgente disciplina del Codice Privacy al GDPR	231
13.4. Gli Organismi di monitoraggio	235
13.5. Le certificazioni	237
14. DATA BREACH	239
14.1. Premessa	239
14.2. Gli elementi della violazione e criteri per determinare l'effettiva conoscenza	240
14.3. Obblighi di notifica	241
14.4. La comunicazione agli interessati	247
14.5. Le procedure interne per la gestione dei data breach	249

I RAPPORTI CON I TERZI

15. I RAPPORTI CON I TERZI	255
15.1. Premessa	255
15.2. I ruoli privacy	256
15.3. Obblighi e responsabilità	269
15.4. Gli accordi	272
16. I TRASFERIMENTI TRANSFRONTALIERI DI DATI	283
16.1. Principi fondamentali e disciplina generale in materia di trasferimenti transfrontalieri di dati	283
16.2. Quando è legittimo il trasferimento dei dati personali all'estero?	284
16.3. I nuovi scenari post brexit	299

I RAPPORTI CON LE AUTORITÀ

17. I POTERI CORRETTIVI DELLE AUTORITÀ DI CONTROLLO E LE SANZIONI	305
17.1. Premessa	305
17.2. I poteri correttivi delle autorità di controllo	305
17.3. Le sanzioni pecuniarie	308
17.4. Le sanzioni e i reati previsti dal codice privacy	313

IL TRATTAMENTO DEI DATI PERSONALI IN SETTORI SPECIFICI

18. SETTORE SANITARIO PARTE I: FINALITÀ DI CURA E PRIVACY	323
18.1. Il dato sanitario	323
18.2. E-health	327
18.3. I dispositivi medici o elettromedicali	334
19. SETTORE SANITARIO PARTE II: RICERCA MEDICA E PRIVACY	336
19.1. Introduzione: la ricerca	336
19.2. La ricerca medica, biomedica e epidemiologica	336
19.3. I dati genetici e la ricerca clinica	344
19.4. Utilizzo successivo dei dati di ricerca	349
19.5. I registri pubblici e privati per il monitoraggio (real life evidence)	350
20. TRATTAMENTO DATI BANCARI E FINANZIARI	354
20.1. Introduzione	354
20.2. Ambito di applicazione del trattamento dei dati finanziari	355
20.3. Diritti degli interessati e portabilità dei dati	357
20.4. Principali Provvedimenti e Linee Guida dell'Autorità Garante per la protezione dei dati personali	360
20.5. Payment Service Directive 2 (PSD2) e l'impatto sul trattamento dei dati bancari	365
21. DIRITTO ASSICURATIVO E PRIVACY	372
21.1. Introduzione	373
21.2. Reti distributive, periti ed altri collaboratori dell'impresa	373
21.3. Data Governance assicurativa: definizione di un sistema di trasmissione delle informazioni efficace	378
21.4. Il trattamento dei dati giudiziari in ambito assicurativo	380
21.5. Il trattamento dei dati di salute in ambito assicurativo: assunzione e gestione dei sinistri	382
21.6. Sistema di prevenzione delle frodi (responsabilità civile auto)	384
21.7. Intelligenza artificiale, big data e settore assicurativo	385
21.8. Diritto di accesso ai dati personali e gestione della fase pre-contenziosa	390
21.9. Antiriciclaggio	391
21.10. Trattamento dati all'interno delle aree riservate	393
21.11. Whistleblowing nel settore assicurativo	395

22. MEDIA & PRIVACY	397
22.1. Premessa	397
22.2. La disciplina applicabile	397
22.3. La tutela dell'immagine in ambito media	399
22.4. I requisiti privacy in ambito media	403
22.5. I diritti dell'interessato	408
22.6. Conclusioni: la centralità del bilanciamento di interessi	410
23. LA PRIVACY NELLE COMUNICAZIONI ELETTRONICHE	
	411
23.1. L'evoluzione della disciplina delle comunicazioni elettroniche	411
23.2. L'ambito di applicazione del titolo X del codice della privacy	414
23.3. Informazioni e dati raccolti nei riguardi del contraente e dell'utente	417
23.4. Marketing diretto e soft spam	422
23.5. Informazioni, conservazione dei dati e sicurezza	425
23.6. Il regolamento ePrivacy: il futuro (prossimo) della normativa sulle comunicazioni elettroniche	427
24. SHARING ECONOMY	438
24.1. Il ruolo della privacy nelle piattaforme della sharing economy	438
24.2. L'effettività del consenso dell'utente al trattamento	443
24.3. La raccolta, condivisione e trasferimento extra-UE dei dati personali	446
24.4. La declinazione dei diritti privacy nella sharing economy: accesso, cancellazione e portabilità	455
25. LA PROTEZIONE DEI DATI PERSONALI NEL SETTORE DEI GIOCHI PUBBLICI	460
25.1. La disciplina dei giochi pubblici in Italia. Il gioco su rete fisica e il gioco a distanza	460
25.2. Gioco pubblico e tutela dei minori	467
25.3. Il contratto di conto di gioco online e la tutela dei dati personali dei giocatori	470
25.4. La normativa antiriciclaggio nel settore dei giochi e la tutela dei dati personali dei giocatori	479
LEGAL TECH E LEGAL DESIGN	
26. LA NUOVA FRONTIERA DEL GIURISTA: IL LEGAL DESIGN	491
26.1. Introduzione	491
26.2. La metodologia applicativa del legal design	492
26.3. Il Design Thinking	496
26.3. Applicazioni pratiche del legal design	497
27. LEGAL TECH E PRIVACY	501
27.1. Il legal tech e l'evoluzione dei servizi legali	501
27.2. Applicazioni della tecnologia alla protezione dei dati personali	502
27.3. Le Privacy Enhancing Technologies	502
27.4. Strumenti legal tech per la gestione degli adempimenti privacy	504

27.5.	Come selezionare gli strumenti legal tech adatti alle proprie esigenze	505
27.6.	Calcolo del ROI sulle soluzioni legal tech	507

FORMULARIO

28.	INFORMAZIONI E DIRITTI DELL'INTERESSATO	511
28.1.	Informazioni sui dati personali presso l'interessato (art. 13 GDPR) - informativa aziende private	513
28.2.	Informazioni sui dati personali raccolti presso soggetti diversi dall'interessato (art. 14 GDPR in vigore dal 25/05/2018) - informativa aziende	516
28.3.	Informazioni sui dati personali (art. 13 GDPR) - informativa enti pubblici	518
28.4.	Informazioni sui dati personali raccolti presso soggetti diversi dall'interessato (art. 14 GDPR) - informativa enti pubblici	520
28.5.	Privacy policy per aziende	522
28.6.	Cookie policy	525
28.7.	Check list di verifica cookie	528
28.8.	Informativa e consenso per newsletter	529
28.9.	Informativa per iscrizione alla newsletter pubblicata sul sito di un Ente	531
28.10.	Informativa sui dati personali per dipendenti e collaboratori....	532
28.11.	Informativa privacy per rilevazione temperatura corporea (emergenza COVID-19)	535
28.12.	Informativa sui dati personali di soggetti che accedono ai locali e agli uffici (emergenza COVID-19)	537
28.13.	Esercizio del diritto di accesso in materia di protezione dei dati personali (art. 15 GDPR)	540
28.14.	Esercizio di diritti in materia di protezione dei dati personali - Modello Garante Privacy	541
28.15.	Dichiarazione di divieto di esercizio dei diritti di cui agli artt. 15-22 del GDPR relativi a persone decedute	543
28.16.	Istanza esercizio dei diritti di cui agli artt. 15-22 relativi a persone decedute	544
28.17.	Reclamo al Garante per la protezione dei dati personali per l'esercizio dei diritti di cui agli artt. 15-22 del GDPR riguardanti le persone decedute	545
28.18.	Esercizio del diritto alla portabilità in materia di protezione dei dati personali	547
28.19.	Istanza di esercizio del diritto alla portabilità dei dati	548
28.20.	Riscontro ad istanza diritto alla portabilità dei dati	549
28.21.	Istanza di esercizio del diritto di rettifica ed integrazione dei dati	550
28.22.	Procedura aziendale per i diritti degli interessati	551
28.23.	Registro delle istanze di esercizio dei diritti sui dati	552
28.24.	Reclamo ex art. 77 del Regolamento (UE) 2016/679	553
28.25.	Segnalazione al Garante	555
29.	FIGURE E RUOLI	556
29.1.	Accordo di contitolarità sui trattamenti di dati personali	557
29.2.	Richiesta del contenuto dell'accordo di contitolarità	562

29.3.	Riscontro a richiesta di accesso al contenuto dell'accordo di contitolarità	563
29.4.	Accordo per il trattamento dei dati da parte del responsabile esterno	564
29.5.	Clausola da inserire obbligatoriamente qualora l'affidamento a Terzi implichi che il trattamento di dati personali debba essere effettuato all'esterno per conto del titolare	571
29.6.	Documentazione delle scelte per la nomina del RPD o DPO (scelta di dotarsi di un DPO).....	581
29.7.	Documentazione delle scelte per la nomina del RPD o DPO (scelta di non dotarsi di un DPO).....	582
29.8.	Schema di atto di designazione del RPD esterno	583
29.9.	Schema di atto di designazione del RPD interno	586
29.10.	Dichiarazione sostitutiva di atto di notorietà - Insussistenza di conflitto di interesse del RPD (Enti pubblici).....	590
29.11.	Istruzioni per comunicazione del nominativo del DPO o RPD al Garante	591
29.12.	Segnalazione di ordine di priorità	592
29.13.	Verifica e aggiornamento delle informative privacy con integrazione del DPO o RPD.....	593
29.14.	Designazione componenti team del RPD o DPO	594
29.15.	Nomina componenti rete addetti di supporto al RPD o DPO...	596
29.16.	Fac simile di relazione sintetica delle attività del RPD o DPO	597
29.17.	Atto di nomina amministratore di sistema.....	598
29.18.	Fac simile di relazione annuale attività dell'Amministratore di Sistema e verbale di verifica del Titolare sulle attività dell'Amministratore di Sistema	600
29.19.	Fac simile di designazione di referente interno	602
29.20.	Autorizzazione ai dipendenti al trattamento dei dati	604
29.21.	Istruzioni autorizzato individuale.....	606
30.	REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO	608
30.1.	Garante Privacy - Registri semplificati delle attività dei trattamenti per le PMI	609
30.2.	Registri delle attività di trattamento del titolare (strutture complesse)	610
30.3.	Registri delle attività di trattamento del responsabile (strutture complesse)	611
31.	VALUTAZIONE DI IMPATTO PRIVACY	612
31.1.	Richiesta di parere sulla valutazione di impatto privacy o Data Protection Impact Assessment (DPIA).....	613
31.2.	Scheda descrittiva allegata alla richiesta di parere al Responsabile della protezione dei dati personali sulla valutazione di impatto privacy o Data Protection Impact Assessment (DPIA)	614
31.3.	Parere sulla valutazione di impatto privacy o Data Protection Impact Assessment (DPIA).....	616
31.4.	Riscontro alla richiesta di parere di valutazione impatto privacy	618
31.5.	Riscontro alla richiesta di parere di valutazione impatto privacy	619

32. VIOLAZIONE DEI DATI	621
32.1. Procedura di data breach	622
32.2. Costituzione di un Punto di contatto informazione su data breach	626
32.3. Nomina addetto comunicazione (Data breach)	627
32.4. Nomina Unità di crisi – Data breach	628
32.5. Violazione di dati personali- modello di notifica al Garante	629
32.6. Comunicazione di violazione di dati personali all'interessato ..	630
32.7. Registro delle violazioni dei dati	631
33. VIDEOSORVEGLIANZA	633
33.1. Modello semplificato cartello videosorveglianza	634
33.2. Informazioni per esteso in relazione all'utilizzo di sistemi di videosorveglianza (art. 13 del GDPR)	635
33.3. Autorizzazione individuale ai dipendenti al trattamento dei dati in relazione a impianti di videosorveglianza	637
33.4. Attestazione fornitore videosorveglianza	639
33.5. Designazione responsabile del sistema di videosorveglianza ..	640
33.6. Scheda censimento telecamere	641
33.7. Richiesta di accesso a videoregistrazioni degli impianti di videosorveglianza	645
34. WHISTLEBLOWING	648
34.1. Informativa	648

INDICI

INDICE CASI	653
INDICE FORMULE	656
INDICE ANALITICO	659